Remarks

In the present paper, Claims 1, 3-8, 20, 22-27, 39 and 41-46 have been amended and new claims 64-72 have been added. Support for the amendments can be found for example, in the applicant's published patent application U.S. Patent Publication No. 2002/0095603, paragraphs 68, 87 and 96, as well as elsewhere throughout the specification. Each of the added claims is dependent upon a pending base independent claim. Support for the added claims can be found, for example, in the applicant's published patent application, paragraphs 73, 74, 97 and 129, as well as elsewhere throughout the specification.

Interview Summary

On August 03, 2006, Thomas Lees on behalf of the applicants, conducted a telephone interview with Examiner Patel. No demonstrations were utilized. Additionally, no exhibits or proposed amendments were transmitted to the Examiner. Claim 1 was discussed in general terms. Additionally, the art of record including U.S. Patent No. 6,411,986 to Susai et al. was discussed. Specifically, the multiplexing and firewall protection taught in Susai et al. was discussed, and applicants' compared and contrasted the disclosure of Susai et al. with the end-to-end security processing described and claimed in the present application, the details of which are further set out in this paper. No agreements were reached between the parties.

35 U.S.C. § 102(e)

Claims 1, 3, 4, 7, 20, 22, 23, 26, 39, 41, 42, 45, 58, 60, 61 and 63 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,411,986 to Susai et al. According to the M.P.E.P. §706.02, in order to be anticipating under §102, the reference must teach every aspect of the claimed invention[1]. Of the rejected claims, claims 1, 20 and 39 are in independent form.

With regard to claim 1, as amended herein, Susai fails to teach or suggest:

routing both inbound and outbound communications with target hosts which are

[1] See also *Carella v. Starlight Archery and Pro Line Co.*, 804 F.2d 135, 138, 231 U.S.P.Q. 644, 646 (Fed. Cir. 1986).

associated with an end-to-end secure network communication through the distribution processor...processing both inbound and outbound end-to-end secure network communications at the distribution processor so as to provide endpoint network security processing of communications ...encapsulating communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications...and distributing the received network communications that are directed to the common network address among selected ones of the target hosts, wherein the selection among the target hosts is carried out so as to distribute workload associated with the network communications among the target hosts.

Remaining independent claims 20 and 39 recite similar limitations.

Susai et al. teaches with reference to Fig. 2, a multiplexer (interface unit) that relieves the processing burden required for a server to repeatedly open and close network connections to clients. In particular, Susai et al. teaches the use of the interface to open one or more connections with a server computer, and maintain those connections open to allow repeated access by clients[2]. In Susai, et al., inbound packets are routed from a client to an intended server through the interface using network address translation as well as connection multiplexing, which translates a packet by modifying its sequence number and acknowledgement number at the TCP protocol level in a manner that requires no application layer interaction[3].

As can be seen with reference to Figs. 4, 6A and 6B, if the packet is an inbound packet, the source network address of the packet is changed to that of an output port of the interface unit and the destination network address is changed to that of the intended server. If the packet is an outbound packet, the source network address is changed from that of the server to that of an output port of the interface unit and the destination address is changed from that of the interface unit to that of the requesting client. The sequence number and acknowledgment numbers of the packet are also translated by manipulating the sequence and acknowledgement numbers to map

[2] See for example, Susai et al. Col. 4, lines 10-16.
[3] See for example, Susai et al. Col. 5, lines 21-36.

to values expected by the recipient[4]. Susai et al. further teaches that the multiplexer may be provided as part of a firewall, router, load balancer etc[5].

However, nowhere does Susai et al. teach or suggest routing both inbound and outbound communications with target hosts which are associated with an end-to-end secure network communication through the distribution processor or processing both inbound and outbound end-to-end secure network communications at the distribution processor as recited in claim 1 as amended herein. Moreover, Susai et al. fails to teach or suggest (and is completely silent with regard to) end-to-end security processing in any sense.

As noted above, and as cited by the Examiner[6], in Susai et al., the interface unit translates the destination and source packets in inbound and outbound messages to route each message between the requesting client and target server computer. However, message redirecting does not teach or suggest processing end-to-end network security communications at a distribution processor.

In this regard, it is noted that the Examiner further argues that the interface unit taught in Susai et al. may be combined with a firewall, and that firewalls monitor packets and allow only the authorized packets to flow through[7]. The inclusion of a firewall with the multiplexer taught in Susai et al. again however, fails to teach or suggest routing both inbound and outbound communications with target hosts which are associated with an end-to-end secure network communication through the distribution processor or processing both inbound and outbound end-to-end secure network communications at the distribution processor as recited in claim 1 as amended herein. For example, security protocols that provide "end-to-end" security provide

[4] See for example. Susai et al. Col. 7, lines 30-59.
[5] See for example, Susai et al. Col. 3, lines 60-67; Col. 13, lines 3-23.
[6] See for example, the Office Action mailed 05/15/2006, pages 3 and 4.
[7] See for example, the Office Action mailed 05/15/2006, page 5 (with regard to Claim 3); Susai et al. Col. 13 lines 15-17.

secure communications for the entire communications path between two host processing systems[8].

Moreover, while Susai et al. does teach redirecting packets by altering source and address information, i.e., functioning as a multiplexer by forwarding packets, Susai et al. fails to teach or suggest (and is completely silent with regard to) encapsulating communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications.

As an example, by encapsulating the communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications, simplified filter policies on the data processing systems may be realized as it may allow for the efficient separation of communications associated with secure network communications from other communications[9].

In view of the amendments and clarifying comments herein, the Applicants respectfully request that the Examiner withdraw the rejections to claims 1, 20, 39 and the claims that depend therefrom under 35 U.S.C. §102(e).

35 U.S.C. §103

Claims 5, 6, 8, 9, 24, 25, 27, 28, 43, 44, 46 and 47 were rejected under 35 U.S.C. §103(a) as being unpatentable over Susai et al. in view of U.S. Patent No. 6,779,051 to Basil et al.

According to the MPEP §706.02(j), to establish a *prima facie* case of obviousness, the prior art reference must teach or suggest all the claim limitations[10]. It is the applicants' position that a *prima facie* case of obviousness has not been established for the claims set out herein as

[8] See for example, paragraph 21 of the Applicant's Published Patent Application No. 2002/0095603.
[9] See for example, paragraph 83 of the Applicant's published patent application.
[10] See also, *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991); MPEP § 2143 - § 2143.03

these claims depend from one of claims 1, 20 or 39, which applicants now believe are patentable over the art of record.

Moreover, cited references, even when combined, fail to teach or suggest all of the limitations of the above-claims as amended herein. For example, the Examiner relies upon Basil et al. for a teaching of the use of a generic routing format[11]. Basil teaches a method of obtaining and forwarding an end point address of a generic routing encapsulation tunnel (GRE) by forwarding end point address information so that GRE tunnels can be automatically updated[12]. However, Basil et al. fails to teach or suggest (and is completely silent with respect to) routing both inbound and outbound communications with target hosts which are associated with an end-to-end secure network communication through the distribution processor. Accordingly, Basil et al. further fails to teach or suggest processing both inbound and outbound end-to-end secure network communications at the distribution processor so as to provide endpoint network security processing of communications.

Also, while Basil et al. discloses generic routing encapsulation in terms of dynamically determining the endpoint of a GRE tunnel, Basil et al. fails to teach or suggest encapsulating communications between the distribution processor and selected ones of the plurality of target hosts which are associated with end-to-end secure network communications...and distributing the received network communications that are directed to the common network address among selected ones of the target hosts, wherein the selection among the target hosts is carried out so as to distribute workload associated with the network communications among the target hosts, as recited in claim 1 as amended herein.

Susai et al., when combined with Basil et al., fail to teach or suggest the claimed invention as set out in greater detail herein. In view of the amendments to the claims and clarifying comments herein, the Applicants respectfully request that the Examiner withdraw the rejections to claims 5, 6, 8, 9, 24, 25, 27, 28, 43, 44, 46 and 47 under 35 U.S.C. §103(a).

[11] See for example, the Office Action mailed 05/15/2006, page 11.
[12] See for example, Basil et al. Figs. 6, 7; Col. 5, lines 10-44.

New Claims

New claims 64-72 have been added herein. Claims 64-66 depend from independent claim 1. In a similar manner, claims 67-69 depend from independent claim 20 and claims 70-72 depend from independent claim 39. The applicants believe that no new search will be required for these claims as each new claim depends from a base claim that is in condition for allowance.

Conclusion

For all of the above reasons, the applicants respectfully submit that the above claims recite allowable subject matter. The Examiner is encouraged to contact the undersigned to resolve efficiently any formal matters or to discuss any aspects of the application or of this response. Otherwise, early notification of allowable subject matter is respectfully solicited.

Respectfully submitted,
Stevens & Showalter, L.L.P.
By

Thomas E. Lees 46,867

7019 Corporate Way
Dayton, Ohio 45459-4238
Phone 937-438-6848
tlees@sspatlaw.com